Information-Based Warfare: A Brazilian Approach to 21st Century

CSC 1998

Subject Area – Topical Issues

EXECUTIVE SUMMARY

Title: Information-Based Warfare: A Brazilian Approach to 21st Century

Author: LCDR Antonio Carlos Chianeli Fonseca, Brazilian Marine Corps.

Thesis: Brazil does not presently have an IW doctrine capable of combating the existing and future threats to its national integrity, and Brazil will be unable to achieve its security objectives without an IW doctrine.

Discussion: Brazilian National Defense Policy considers border control and drug traffic as major threats for Brazilian security. The region most vulnerable to those threats is the Amazon. The Brazilian Amazon is considered an excellent way to allow drug traffic and cultivation. Drug traffickers use Brazilian territory to dispatch drug to consumer's center, inclusive US. That situation must be controlled for the next century. To solve the problems of border control and drug traffic Brazil has many approaches, but based on Brazilian Strategy, historical characteristic of peaceful nation, and resources' availability, the less expensive approach is the establishment of an IW doctrine for the year 2000. To do it, IW must be considered as an efficient tool to Brazil's strategy, and the legal, technological and intelligence environments must adequate to a new situation. Finally, beyond strategic evaluations, some operational changes must be considered, such as the Brazilian Marine Corps' Information Warfare independent company which would be responsible for IW analysis and employment during peacetime or crisis.

Recommendation: Brazil must consider the IW doctrine proposed in order to achieve economically its National Defense Policy objectives of border control and drug traffic.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **1998**	2. REPORT TYPE	3. DATES COVERED **00-00-1998 to 00-00-1998**

4. TITLE AND SUBTITLE **Information-Based Warfare: A Brazilian Approach to 21st Century**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps,Command Staff College, Marine Corps University,2076 South Street, Marine Corps Combat Development Command,Quantico,VA,22134-5068**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**47**	

CONTENTS

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

Table **Page**

INFORMATION-BASED WARFARE A BRAZILIAN APPROACH

TO THE 21ST CENTURY

Most of today’s techno-rebels are neither bomb-throwers nor Luddites. They include thousands of people who are themselves scientifically trained - nuclear engineers, biochemists, physicians, public health officials, and geneticists as well as millions of ordinary citizens. Again, unlike the Luddites, they are well organized and articulate. They publish their own technical journals and propaganda. They file law-suits and draft legislation, as well as picket, march, and demonstrate.

This movement, often attacked as reactionary, is actually a vital part of the emerging Third Wave. For its members are the leading edge of the future in a three-way political and economic battle that parallels, in the field of technology, the struggle over energy that we have described earlier.

Alvin Tofler, The Third Wave

The Information Warrior is not as rare as a flood, or as benign as an ice storm. The Information Warrior is not a natural catastrophe, an act of God, or Mother Nature getting even with man. The Information Warrior creates well-planned man-made disasters with all contingencies considered, all alternatives explored, and all escape plans evaluated.

Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway

Brazilian armed forces must prepare for the next century by applying a greater share of available resources in order to develop the information based capability needed for an emerging power. To do this, the Brazilian military forces need to formulate an Information Warfare (IW) doctrine which matches the Brazilian National Defense Strategy.

The central argument of this thesis is that Brazil will be unable to achieve its security objectives without an IW doctrine. The paper will show that Brazil does not presently have an IW doctrine capable of combating the existing and future threats to its national integrity, and will propose a model to fill in this doctrinal gap. The essay will trace development of Brazil's technological advances in the telecommunication field, and analyze its response to the threats it is likely to face in the next century.

First, this document will introduce a historical background of Brazilian IW improvements. After historical considerations, it will present Brazilian National Defense Strategy and its relationship to IW, taking into account the Brazilian armed forces involvement, specifically the Marine Corps. Brazil's IW doctrine properly stated follows, with considerations and practical actions to be adopted in accordance with Brazilian Strategy. Finally, some recommendations for new doctrine will be related and linked with Brazil's strategic relationship with the United States and South America.

Technology improvements in telecommunication systems have had a revolutionary impact on this century. The effects of connecting the entire world are infinite. Satellites, submarine fiber optic cables, and complex systems of radio links in various frequency bands are among the investments made to satisfy final user. Today, technology is directly related to microprocessors. Huge components that permit great speeds of processing due to increased internal memory, processing capacity, and clock frequency, are the engines for continuous technological development. However, the augmentation of processing speed presents new problems to the developers. Since the 1980's, the microprocessors' clock frequency increased by a factor of 30, giving them the classification of radio transmitters and receivers. The emission of frequency outside the processor influences the copper strips, introducing undesirable capacitance generating disturbances into the system, and allowing it to be more vulnerable to external frequency interference.

The continuous increase in information flow has directed efforts to develop more efficient interconnection systems. When the magnitude of connections increases, it is necessary to develop faster protocols that enable these connections to integrate logically. State-of-the-art protocols can empower speeds of connection on the order of billions of information units per second. From theory to practical life - what type of physical connection between systems will be used to support this rate of information flow? Have communication protocols developed beyond the physical connection possibilities? And who will need systems with more speed than is available today? Is technological advance in microprocessors a requirement for improving the effectiveness of military organizations?

Thus, knowledge is the key to the future. The dissemination of computer and telecommunication information to everyone interested is emerging as a major threat in the next century. How is it possible to control the flow of sensitive information within governmental and military offices? To attain greater efficiency, system developers often ignore security. During development, that procedure wastes time, and security control often reduces processing speed when it uses part of the processor's duty cycle to execute tasks different from the objective ones. Those who have the ability to develop an efficient system can develop a secure system, and can develop a means of bypassing security and gaining access to the system controls. In "Masters of Deception",[1] teenagers gained access to telephonic computer systems with the initial purpose of learning how it works - basically, to get knowledge not easily accessible to someone. The curiosity of human nature and its characteristic desire for control led them deeply inside the telephonic systems where they gained the ability to change sensitive information in what ever way they wished. Knowledge and control of information are real threats for a new era.

[1] Michelle Slatalla and Joshua Quittner, *Masters of Deception: the Gang that Ruled Cyberspace* (New York, NY: HarperPerennial, 1996).

BACKGROUND

During the past 20 years, Brazil, with its great territorial expansion and internal problems related to police and control, has been used as an efficient pathway for drugs coming from other South America countries, with the objective of reaching drug consumers and distribution centers around the world. More than 50 % of the country has forest and jungle borders with other South American countries, which facilitates access to Brazilian territory to produce or dispatch drugs without interference from the governments of those countries.

For over a century, Brazil has not been involved in a conflict with any of its neighbors, which gives it international recognition and credibility, but the existence of some zones of instability in the region have focused Brazilian consideration of possible threats that could develop around its boundaries.

> The current problems existing in the arc of the Amazonian border from French Guyana to Bolivia, involve the management of Indians, clandestine mining, and the smuggling of precious minerals, contraband and arms. The root of the problems can be linked to the strong connection between foreign guerrillas and drug traffickers which create the phenomena of narco-guerrillas (particularly in Peru and Colombia). This situation presents the possibility of escalating crises which have the potential to unleash threats to the vital interests of Brazil in the Amazon. This especially concerns the sovereignty and the territorial integrity of the national patrimony.[2]

Despite having the same thoughts as the United States for combating the narco-traffic and maintenance of a peaceful America continent, Brazil has many differences in approaching the challenges to accomplish those thoughts, including the military

[2] Álvaro de Souza Pinheiro (Col-EB), *Guerrilha in the Brazilian Amazon*, (Fort Leavenworth, KS: Foreign Military Studies Office, 1995), 18-19.

governmental structure and the border control policy.

Due to the historically peaceful tradition of Brazil, the United States considers it an important partner with respect to the stabilization and security of the American continent. The employment of an IW doctrine will strengthen the military relationship between Brazil and United States with the mutual exchange of secure knowledge and experience. Drug enforcement and international crime organizations - the major threats to Brazilian National Defense - are also concerns of the American government, and a multinational force to combat these threats could be built in the next years.

> Brazil is faced with a series of problems deriving from drug abuse, which regard production, commercialization and transit of licit and illicit psychoactive substances, besides the menacing underlying violence and criminality that is connected to the issue.[3]

With adoption of IW doctrine presented, Brazil-US relations will increase and Brazil must prepare to absorb international implications derived from that partnership. Since drug cultivation is an illegal part of economic resources for some South American countries, combating drug traffic inside Brazilian territory will reduce drug consumption - as expected - and will directly interfere in criminal organizations interests. All South American countries, except Guyana, have signed international drug control treaties, which shows that drug enforcement is a concern of almost all South American nations, and Brazil-US cooperation in drug enforcement would be considered more beneficial than prejudicial to South American interests.

> A large majority of the illicit drugs which enter the United States originate in Latin America and the Caribbean region. Virtually all of the world's cocaine and most of the marijuana comes from Latin America and the Caribbean. While Asia remains the principal source of heroin, South America is now providing a

[3] Ministry of Justice Brazil, *National Drug Enforcement Program* (Brasília, DF: Ministry of Justice, 1996), URL: <http://www.brasil.emb.nw.dc.us/wpar09dr.htm>, accessed 2 January 1998.

significant percentage of high grade product. South American heroin is distributed nationwide in large part by the same trafficking network that distributes cocaine.[4]

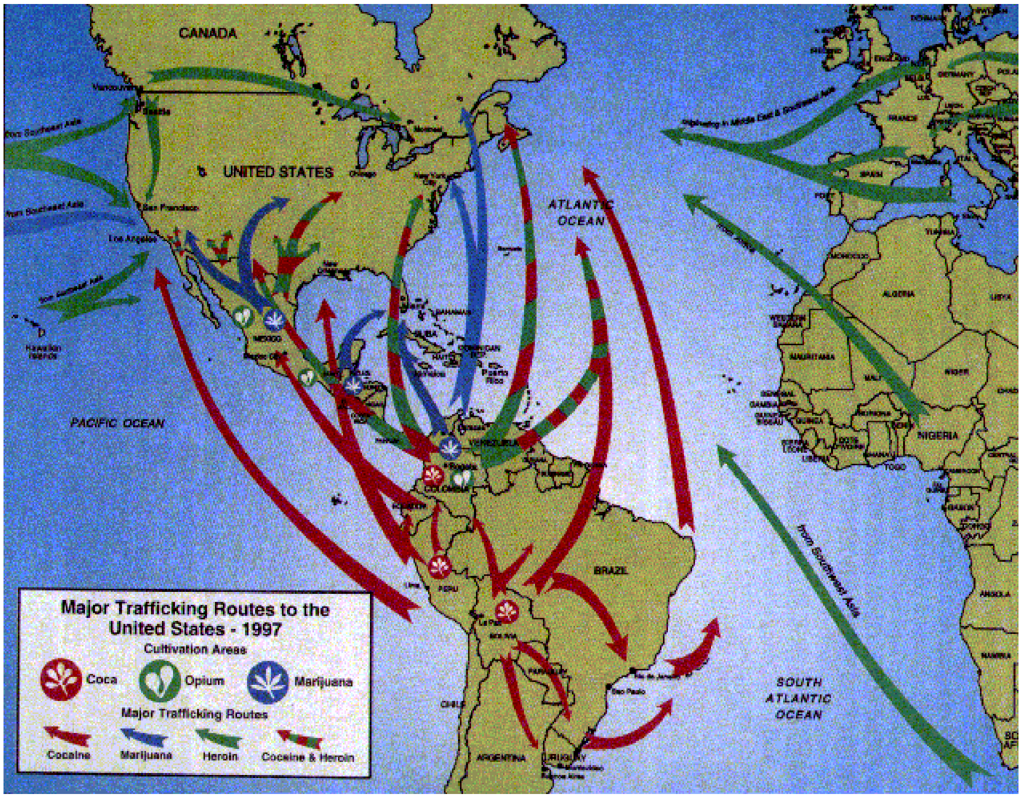

Figure 1. Major trafficking routes to US

Source: William W. Mendel and Murl D. Munger, “Major trafficking routes to US,” *Strategic Planning and the Drug Threat,* (Fort Leavenworth, KS, Strategic Studies Institute, 1997), 6.

Unfortunately, different from the American model, the actual Brazilian governmental structure, which establishes a direct relationship between the President of Republic and the Ministers (including the military ones) inhibits integration between ministries. In fact, it happens between all the ministries, not only among the military

[4] William W. Mendel and Murl D. Munger, *Strategic Planning and the Drug Threat* (Fort

(Army, Navy and Air Force). Each ministry has its own grievances and integration sometimes means distribution of resources to areas of importance not directly related to each ministry's independent policy.

Due to the differences of approach by each ministry, there are multiple telecommunication and information systems running over a complex diversity of equipment. These systems are extremely old or belong to the electronics state-of-the-art. Some services developed exclusive equipment for specific purposes (stove-pipes) while other services use commercial, off-the-shelf systems (COTS).

In terms of IW, Brazil's resources were applied to development of internal networks for specific agencies and branches of the government and to acquire basic military equipment to be applied to detection (radar and sonar), communications (encryption systems), and weapon control systems. With digitalization of governmental databases, internal networks needed to establish interconnection with others and secure communications structures had to be built to allow the flow of information. In fact, the development of network integration and security was improved in accordance with each ministry approach to the situation.

Within the differences of approach, a fact that imposes discontinuity of efforts among the military ministries, is the difference of objectives and areas of action. Each armed force developed its own telecommunication doctrine independently of the others. Similar to the United States, there are interoperability problems within Brazil's armed forces. The problems multiply during mixed exercises when the Navy cannot synchronize its effort with the Army and the Air Force; especially in fire support coordination due to

Leavenworth, KS: Strategic Studies Institute, 1997), 5.

the existence of non-standard equipment in use.

The coordination problems are worst when the issue of regional cooperation between Brazil and other countries arise. For example in the Amazon region in 1991, a group of Colombian guerrillas attacked a Brazilian Army detachment. To avoid other attacks and to ensure security in the region, the governments of Brazil and Colombia developed a binational combined operation in the limits between the countries, named "Traira Operation."[5] This operation involved the Colombian Army and the three Brazilian armed forces, some of them with detachments from different regions of Brazil, including the recently-created Brazilian Army Aviation. Despite the successful results of the operation, there were problems in establishing interoperability among the forces involved in the operation: the age of equipment in operation compared with the one used by the forces in different regions or because Amazon is not the easiest place to establish a reliable information and communication network. After the solution of the communication problems, the operation could begin, and the Brazilian armed forces learned a lesson, at least with respect to the achievement of multinational communication integration.

As stated above, an IW doctrine which enhances the establishment of interoperability and gives an anticipated threat warning to the forces deployed inside the country is a prerequisite to control of the Amazon Basin. The movement toward the west was different for Brazil. It stopped in the jungle, a region more dangerous to explore than the central American deserts, and due to lack of settlements on the Amazon region, the Brazil's National Defense Strategy evolved differently from America's as will be

[5] Pinheiro, 15.

addressed in the next chapter.

BRAZIL'S NATIONAL DEFENSE STRATEGY

To better understand the differences and similarities between US and Brazil strategies, some analysis is needed. The US Military Strategy - Shape, Respond, Prepare Now - uses strategic agility, overseas presence, power projection and decisive force concepts[6] to achieve the full spectrum dominance established in Joint Vision 2010. The same concepts could be employed by Brazil's Strategy, but they require a different scale of approach. Due to the large dimensions of the country, low availability of economic resources to invest in military improvement of equipment and personnel, and the established tradition as a peaceful nation (defensive posture), Brazil can neither establish an overseas presence nor project force outside the country. For Brazil's strategy, it is time to maintain the nation's sovereignty and counter threats to economic and social stability.

> Large-scale illicit coca bush cultivation continues in Bolivia, Colombia and Peru. Peru remains the largest producer of coca leaves and Colombia is the second largest. Illicit cultivation of the epadú variety of coca bush seems to be increasing in Brazil, mainly in areas that are close to its borders with Colombia and Peru.[7]

As stated in the Brazilian National Defense Policy, the armed force's mission is *defending the Nation, whenever necessary, ensuring the maintenance of its territorial integrity and sovereignty.[8]* As a warfighter, together with my service experience, I believe that the Brazilian government can more capably and economically defend itself

[6] Shalikashvili, John M., Chairman of the Joint Chiefs of Staff, *National Military Strategy of the USA* (Washington, DC: Pentagon, 1997), 3.

[7] International Narcotics Control Board, *Report of International Narcotics Control Board for 1997* (Vienna, Austria: United Nations Publications, 1998), URL: <http://www.undcp.org/incb/AR/e/report.htm>, accessed 3 January 1998.

[8] Fernando Henrique Cardoso, *Brazilian National Defense Policy* (Washington, DC: Brazilian Embassy on the United States, 1996), URL: <http://www.brasil.emb.nw.dc.us/fpst10de.htm>, accessed 2 January 1998.

against illegal territorial invasion with direct investments in IW. Instead of the Brazilian historic characteristic of diplomacy and its natural defensive posture, the armed forces would be prepared to achieve the national objectives using an information-based warfare doctrine to ensure internal stabilization, boundary control, and drug and crime enforcement.

> Aided by enhanced surveillance capabilities in the form of unmanned aerial vehicle, airborne radars, and satellites, fewer armored and air-mobile ground forces can now concentrate the effects of combat power against the enemy. Rather than move to contact, "all arms" units electronically search and then destroy the enemy on the battlefield.[9]

IW, as a strategic component, is another tool available to military forces in war and, despite its technological capability, nations will always need to deploy ground forces in order to win wars. The technological improvements are directed to allow more effective employment of ground forces to defeat the enemy. Physical contact will still exist during war, but with a different perspective driven to less casualties and loss of time, allied to increased tempo to accomplish the mission.

> The actions of armed groups that are active in neighboring countries, on the edge of the Brazilian Amazon, as well as international organized crime, are among the points that cause concern.[10]

As stated above, Brazil recognizes the primary threats as the possible continuation of external conflicts from other countries in its territory, such as guerrillas (*e.g.*, Sendero Luminoso - Shining Path) that could change the actual relative peaceful panorama to an unstable one, and the international organized crime menace, basically drug traffic. More important than establishing an external deployment overseas, the Brazilian government considers the achievement and maintenance of such international concepts as

[9] Douglas A. Macgregor, *Breaking the Phalanx: a New Design for Landpower in the 21st Century*

sovereignty, self-determination and national identity, which are presented as major targets to threats formerly stated.

The development of a Brazilian IW doctrine will contribute to law enforcement against the threats related in Brazilian Defense Strategy, which are concerns of the entire international community. Also, the Brazilian IW doctrine will help the achievement and maintenance of the Brazilian National Defense Policy objectives, which are:

> a. to guarantee sovereignty while preserving the Nation's territorial integrity, heritage and interests;
> b. to guarantee the rule of law and democratic institutions;
> c. to maintain the Nation's cohesion and unity;
> d. to protect the individuals, goods and resources that are Brazilian, or under Brazilian jurisdiction;
> e. to achieve and maintain Brazilian interests abroad;
> f. to give Brazil a significant role in international affairs and a greater role in the international decision-making process; and
> g. to contribute to the maintenance of international peace and security.[11]

Among the directives to accomplish these objectives, the following are related to the IW doctrine and the military society:

> a. Take actions to maintain a climate of peace and cooperation along all of Brazil's borders and to foster solidarity within Latin America and in the South America region;
> b. Maintain the participation of the Armed Forces in support activities with the aim of national integration, civil defense and the social and economic development of Brazil, in harmony with their constitutional mission;
> c. Protect the Brazilian Amazon, with the support of all of Brazilian society, and with a high value given to the military presence;
> d. Give priority to actions for the development and reinvigoration of the strip of land along Brazil's borders, especially in the northern and central western regions;
> e. Improve the organization, matériel, training, and coordination of the Armed Forces, ensuring that they have the wherewithal, the organizational means and the professionally-qualified personnel to fulfill their constitutional mission;
> f. Enhance the command, control and intelligence capabilities of all entities involved in national defense, providing to them means to facilitate the decision-

(Westport, CT: Praeger, 1997), 49.

[10] Cardoso.

[11] Cardoso.

> making process, both during peacetime and in situations of conflict;
> g. Enhance the system of surveillance, control and defense of Brazil’s borders, airspace, continental shelf, and the waters under its jurisdiction, as well as maritime and air traffic;
> h. Strengthen the national transportation, energy and telecommunication systems;
> i. Seek a level of scientific research, technological development and production capacity that will minimize this country’s dependence on foreign sources for strategic resources that are needed for its defense;
> j. Promote scientific knowledge of the Antarctic region and an active Brazilian participation in the decision-making process about its future;
> k. Enhance the Mobilization System in order to meet this country’s needs, when forced to become involved in an armed conflict.[12]

To achieve these national objectives, Brazilian society would integrate its efforts in all fields, especially with respect to information security, national internal surveillance and boundaries invasion evaluation.

The first step in the integration of efforts toward a national security directive to accomplish the objectives relative to the Amazon Basin, was creation of SIPAM/SIVAM (System of Amazon Protection - Amazon Surveillance System)[13]. This system was designed to integrate the less-controlled regions of Brazil into a telecommunications satellite network, which would permit the evaluation of narcotic traffic and criminal invasion throughout national boundaries. This necessity came from the Brazilian Federal Police’s lack of personnel needed to control the boundaries and perform their National Defense objectives. The SIVAM was designed to work with another system – CINDACTA (Integrated Center of Aerial Defense and Aerial Traffic Control) – which is the responsibility of the Air Force. In spite of the efforts of SIVAM, that system was specified and bought by only one ministry. The necessity of integration with other ministries was taken into account, but the integration will be compromised since each

[12] Cardoso.

[13] Daílson M. de Oliveira (TCol-Av-FAB), *SIPAM-SIVAM. Olhos para a Amazônia* (Montgomery, AL: Airpower Journal International - Portuguese Edition, 1995), URL:

ministry works independently.

Another telecommunication system which will permit integration of the military effort, is the SISCOMIS (Military Satellite Communication System). This system was designed by all the military forces and the communications ministry. Its structure was developed with constant technical and administrative representation of each military force. The basic purpose of the system is the telecommunication integration of the Brazilian Military Structure of War for voice, data and image information exchange[14]. A multiple service commission is empowered to control the development of the system, and the acquisitions for it. However, problems persist, the equipment will be acquired and controlled by each military branch inside its own area of influence (today the system has three earth stations to establish communication with the Brazilian satellites, with each of the stations belonging to one of the branches). The logistical problems are great once each force applies its resources in accordance with its individual needs. The technical committee presents the best efforts toward integration, but the rapid evolution of technology and the slow rate of acquisition normally surpass those efforts.

Security, as currently designed, is greatly compromised. The system utilizes part of the Brazilian commercial satellite system to communicate, and the wire system runs over the public system, across streets or sharing multipurpose cables. This procedure permits interference, restricts the security level of information, and the system loses credibility. To fix this problem, the technical committee is studying the application of encryption solutions to the system. However, the costs of this evolution will compromise the network's security by the creation of hierarchy levels that deserve more security than

<http://www.edsar.af.mil/apj-p/poliveira.html>, accessed 3 January 1998.

others, *i.e.*, within the same network, some users will be allowed to use encryption equipment while others will not.

The use of public and commercial systems to communicate also has an advantage, but a dangerous one. To direct and physically attack military systems, the attacker will have to know which cable is used by the system he wants to threaten, and it will cost time. However, if time is important - for example, to avoid a rocket launching with military satellites - it would not be a problem for the attacker to cut off all communications, civilian or military, that flow through that cable network. In that case, the results will be more extensive and would affect all Brazilian society sectors with unmeasurable consequences.

There is a project to integrate all systems – SIVAM, SISCOMIS, and CINDACTA. The first phase of this integration will be the acquisition and installation of a new earth station to mutually serve SIVAM and SISCOMIS, based in Manaus city. In addition, with the natural integration of the SIVAM and CINDACTA with respect to aerial space defense and control, the integration of the systems will be physically and logically done. The challenge is in evaluating the implications to the telecommunication traffic among the systems with respect to their different basic purposes. All the systems will collaborate with Brazilian national security, but the prioritization of utilization is a challenge to be developed in the next few years.

Another capability being considered to accomplish Brazil's security objective of controling the Amazon region is the operational military occupation with forces capable of rapid deployment within the region. As a Navy component, Brazilian Marine Corps

[14] The author was the Navy Technical Manager for SISCOMIS until June 1997.

(BRMC) is prepared to conduct force projection operations in order to contribute in the achievement of National Defense Strategy objectives. Differently from USMC, and based on Brazilian Strategy, BRMC has the capability of force projection only inside Brazil's territory where there are areas still unknown and which are targets of many threats. BRMC deployment all over the country allows the establishment of a fast and effective force trained in various environments, and capable of accomplishing a diversity of missions, from special operations to conventional ground operations, beyond its traditional amphibious characteristic.

In the Amazon Basin, the most threatened area for the Brazilian Defense Strategy, BRMC has two Battalion-sized units, one in the city of Manaus (Amazon state) and another in the city of Belém (Pará state). Those two units are well-trained and prepared to be employed in any operation inside the region, especially riverine and counterdrug operations.

Finally, information which gives advanced warning to potential threats to Brazil's defense community, inside its area of interest, are necessary. As an example of this concern, President Cardoso recently approved legislation which allows the destruction of aircraft which invade Brazil's National Air Space. "The President approved an important law to combat traffic of drugs, which is fundamental for public security. Brazil is building the elements necessary to eliminate the escalation of drug traffic"[15]. From that raises the necessity to develop an IW doctrine capable of permitting an efficient military response to threats against Brazil's National Security. Due to Brazil's tradition, the focus of this

[15] Adriana Vasconcelos, "FH sanciona lei sobre derrubada de aviões." *O Globo on-line*, 16 Jan

1998, sec. País, URL: <http://www.globoon.com.br/pais/19980116.htm>, accessed 16 Jan 1998.

doctrine will be defensive, but it must also consider a possible IW offensive posture. The drug threat identified in Brazilian National Defense Policy can be seen as a domestic problem, but for Brazil it is a major concern when compared to the US.

INFORMATION WARFARE DOCTRINE (PROSPECTS AND PROBLEMS)

Brazil's concept of IW is still very immature and, despite efforts to improve, does not have a doctrine which comprises the major environments of its society. To start the development of doctrine, Brazilian capability must be compared to that of other nations. The world's leading nation in IW, due to its large-scale computer development, production and utilization, is the United States, which defines IW as

> actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. [16]

Actually, Brazil does not as yet have an IW definition, but based on commonality of existing systems, the above definition should be considered as a model for the Brazilian one:

> Information Warfare consists of the defensive and offensive activities developed to establish an environment that can be controlled, administered and managed with respect to one or more threats against a specific system.

The Brazilian IW definition encompasses all battlespace functions (Command and Control, Intelligence, Fires, Maneuver and Movement, Logistics, and Force Protection) proving its validity for military application. Its connection to Command and Control is obvious. Based on its proper name, IW has a synergistic relationship with Intelligence. The influence on enemy systems and the denial of information to the enemy are fundamental principles of intelligence, and can be achieved with the establishment of a

[16] Directorate for Command, Control, Communications and Computer Systems report (J-6 report), *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, (Washington, DC: Pentagon, 1996), B-76.

reasonable environment which allows the execution of intelligence-related activities. The main purpose of the activities derived from the Brazilian knowledge and technological advance is the establishment of temporary information superiority, at least sufficient to defend specific national objectives from the enemy threat.

The activities developed against the enemy threat can be considered non-lethal fires. The desired effects caused by an IW attack are the same: denial, neutralization and destruction. The target of IW attack can be enemy weapons systems or command and control systems, and the effects could be more effective than a direct attack from destructive fires since most modern weapon targeting and C4I2 systems rely completely on technological control.

> Armies have always used information technology - smoke signals in ancient days, telegraphs at the turn of the century, precision-guided munitions today - but until recently information systems were second in importance to “real” weapons, such as tanks, aircraft, and missiles. Today, information systems are so critical to military operations that it is often more effective to attack an opponent’s information systems than to concentrate on destroying its military forces directly.[17]

Also, within the offensive and defensive activities developed, deception is one which influences maneuver when it gives the enemy false information related to the friendly maneuver intention or movement. Another example is saturating part of the battlefield by jamming and electronic warfare measures, a type of shaping that leads the enemy to avoid that part of terrain, due to the difficulties in controlling and communicating with subordinate elements.

To validate Brazil’s IW definition, logistical improvements must be made in order to sustain Brazil’s capability to maintain and control a friendly environment. The

[17] Bruce D. Berkowitz, “Warfare in the Information Age,” in *Information Age Anthology*, ed.

management of the radio frequency spectrum is an important tool for accomplishing the logistical mission. This management must consider enemy requirements for establishing its communication and capability to interfere in the friendly ones, and the friendly use to establish military and civilian communications, to gather information from the enemy and to interfere in the enemy's capabilities.

The Brazilian definition shows that both offensive and defensive activities are important, which highlights force protection. In accordance with Brazilian defensive posture, IW offensive activities can not be placed above the national system's security. Defense of Brazil's national systems is paramount because the reliance on technologically advanced systems is unavoidable. Using the United States as an example, it is improving the defense of its systems based on the Joint Staff definition of Information Security:

> The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.[18]

The United States gives importance to the eventuality of an asymmetric information attack.

> As the United States becomes more dependent on computerized information systems, and the links between these networks grow, so does the vulnerability to an electronic assault that could paralyze the country.....U.S. intelligence agencies estimate that potential adversaries are not likely to acquire the capability to execute such attacks [invasion of military and major commercial computer networks] for some years. But intelligence officials also have noted that the devices that would be used in cyber attacks - destructive computer software like "logic bombs" and "viruses", or advanced hardware like high-energy radio frequency devices and electromagnetic gear - already are available.[19]

David S. Alberts and Daniel S. Papp (Washington, DC: National Defense University, 1997), 523.

[18] J-6 report, B-76.

[19] Bradley Graham, "11 U.S. Military Computer Systems Breached by Hackers This Month," *The Washington Post*, 26 February 1998, sec. A1.

The quote above is related to hacker attacks on U.S. military computer systems during the U.S. deployment of troops and equipment to the Persian Gulf in 1998. If the target was not U.S., but Brazil's military computer systems, how could Brazil cope with this problem? Perhaps, the attack has already happened and nothing was done to avoid this. Based on this perception, Brazil should start the development of an IW defensive base, which will protect Brazilian systems against the threats of the future. When the technological advances are so fast that it is difficult for most servicemen to keep pace, the possibility of an improper use of the system could be as prejudicial as a real enemy attack.

> What stands clear today is that information technology has reached critical mass. Information systems are so vital to the military and civilian society that they can be the main targets in war, and they can also serve as the main means for conduct offensive operations. In effect, IW is really the dark side of Information Age. The vulnerability of the military and society to IW attack is a direct result of the spread of information technology.[20]

Using one of the main threats to Brazil's National Defense - narco traffic - it can be assumed that, after the establishment of communication systems to integrate Amazon's defense, electronic activities can be employed by narco traffickers in order to blind national defense systems and allow the use of Brazilian territory to transport drugs. The defensive posture adopted in Brazil's National Defense Policy must consider the capability of an offensive IW reaction to that kind of menace.

As an effective military action, sometimes attack is the best way to protect, or defend, the force involved. In that case, Brazilian IW doctrine might assign activities to establish the defensive against an attack on its information infrastructure, and take the

[20] Berkowitz, 529.

offensive when necessary.

The Brazilian information infrastructure consists of technology, networks, information and telecommunication systems. Other infrastructures are important in the evaluation of the information infrastructure as they have direct impact on the maintenance of the operating systems, such as electrical power. Today, due to the information infrastructure complexity and interdependence, it is impossible to recognize where one network ends and another begins.

RECOMMENDATIONS AND CONCLUSION

In order to propose an IW doctrine suitable for Brazil, it is important first to determine the necessary changes to important environments of Brazilian society. The Brazilian information infrastructure for the next century will be a vital component of any IW strategy or policy. This infrastructure has to be modeled in accordance with the legal, technological and intelligence environments. The efficiency of any IW doctrine proposed is directly related to the successful preparation of each of those environments.

Crimes against information systems have to be considered by the Brazilian Congress as a special case where an independent legislation has to be developed. Despite little knowledge of the issue by the legislators, the responsibility has to be addressed by them, not by the technicians. A few years ago, the government created a committee to investigate and to control the use of the Brazilian Internet[21]. Some technical and commercial rules were developed, but the legal aspects were left behind. It happened because the major members of the committee were technical experts. To correct this, the first step is to develop a consistent IW doctrine while simultaneously integrating the legal and technical efforts with the objective not to censor the access to information, but to rule the uses and abuses committed. As an example, with little search effort the Internet gives all the information needed to find anyone inside America, including the telephone number and address of important government members. The consequences of improper use of this information are unlimited.

The legal environment will address not only the regulatory laws, but mainly the

[21] Committee for Brazilian Internet Management.

punishment related to information crimes. The theft of information from any database - paper or electronic - might be considered a crime against privacy. For any information-related crime, there is one similar within the Brazilian crime enforcement law. It is just a case of shaping the actual legislative system in accordance with the information related crimes.

> Because modern societies are themselves so dependent on information systems, often the most effective way to attack an opponent is to attack its civilian information infrastructure - commercial communications and broadcasting networks, financial data systems, transportation control systems, and so on. Not only is this strategy more effective in crippling or hurting an opponent, but it often has some special advantages of its own.[22]

As an example, if an IW attack against the electrical power system control could affect a hospital's function, and due to this action some people die because it was impossible to care for them without electrical power, then the attacker has to be accused of unintentional murder, i.e., in case his assumed objective was other than the hospital. But this issue is not part of the concern of one isolated nation. As stated by Major Aldrich, "Information Warfare takes place in what has come to be known as cyberspace, an ethereal place that does not neatly fit into the land, sea, air, space dichotomy. Information warfare involves conduct and effects that transcend national boundaries and render such distinctions superfluous."[23] The international legal environment has to be prepared to respond to domestic and international information related crimes. Brazil's legislation branch must address the issue as soon as possible to serve as an example to other nations.

The technological environment is the most difficult to shape in accordance with

[22] Berkowitz, 523.

[23] Richard W. Aldrich, Maj (USAF), *The International Legal Implications of Information Warfare*, (Montgomery, AL: Airpower Journal, Vol X No. 3, 1996), URL:

the world’s evolution. It can be treated differently with respect to education, research, and employment aspects. Each of these aspects will be considered in order to avoid interfering in the legal and intelligence environments.

In the particular case of technological education, the Brazilian IW doctrine must be taught early, including the problems related to its deviation from the requirements established by law. The basis for IW education is the enhancement of knowledge for future information age specialists. The next century will be full of good and bad examples related to the information infrastructure. The understanding of a doctrinal security policy is the major concern to be developed for the maintenance of Brazilian defensive strategy. One well-secured network is the key against IW threats in the future.

The technological research community should concentrate its efforts on identifying measures to secure and defend information systems against external threats. The constant investment in education and the support of research will aid the establishment of a secure environment to achieve Brazilian national objectives. The purpose of enhancing education and research investment is not aimed only at acquiring knowledge abroad, but to enable Brazilian experts to develop adequate information quality in accordance with the nation’s needs, capacities and policy.

The employment of Brazilian technological resources in IW has to be related to the appropriate threat level against the national information system. The “Four Levels of Threat” table presents a good guide to the technological employment.

During President Fernando Collor de Mello’s term, the Brazilian intelligence community was seriously shaken by the deactivation of special intelligence agencies

<http://www.cdsar.af.mil/apj/aldricha.html>, accessed 25 August 1997.

responsible for information acquisition and analysis for the government.

threat level	example of threat	actions to be employed
1	no threat - peacetime	defense and enhancement of security activities
2	invasion of information systems for read only purposes	search and accompaniment of the invader, plus actions of threat level 1
3	invasion of information systems for corruption or illegal use of data; virus infection	information countermeasures, isolation of invaded system, plus actions of threat level 2
4	invasion and threat to military and high governmental echelons information systems for any kind of activity - wartime	information countermeasures, isolation of every external communication with the system invaded, plus actions of threat level 3

Table 1. Threat level definition

For the development of a Brazilian IW doctrine, the intelligence environment might be reconstituted and enhanced with specialized training for agents and analysts. Specialized training means development of intensive and objective training in order to provide the intelligence agents and analysts capabilities to collect, gather, analyze, and disseminate information, to conduct deception and psychological operations, and to react against an IW attack.

> The electronic battlefield will create new training challenges. Our [American] forces must be trained to operate efficiently both with and without new technology. They must be able to utilize fully the information provided by technology, but they must also continue to operate if their equipment is rendered useless. Training must not ignore basic skills, even when the environment relies upon technology.[24]

President Fernando Henrique Cardoso started the reconstitution of the intelligence community with the creation of the National Intelligence Agency with the same tasks and purposes of the former agencies. For a concrete IW doctrine, the concentration of effort in a single intelligence agency is only valid if it can effectively control and manage all ministries' intelligence agencies, including the military ones. The bias of intelligence as a military issue has to be surpassed with the agreement that all ministries can best identify their own functions, but the general control of this kind of activity can be executed by personnel without intensive military training. A good example to be followed is the American Central Intelligence Agency (CIA).

action	threat level of application	activities related to the action
deter	all levels	• develop training and education programs; • establish management control of information; • develop capabilities to protect, detect, restore and respond to a threat; and • allocate necessary resources to execute the activities above.
protect	all levels	• develop and implement plans for risk management; • secure friendly information vulnerabilities; and • employ advanced technology.
detect	2, 3 and 4	• provide detection of intrusions and attacks against information databases.
restore	3 and 4	• warn users and operators about threat level development; • reallocate key infrastructure services to critical functions; and • restore the infrastructure to its full operational capability.
respond	3 and 4	• confirm the nature and severity of attacks for proper response; • exploit the enemy information vulnerabilities; and • explore the range of options in the legal, technological and intelligence environment: civil and criminal prosecution, employment of military force, information persuasion, and diplomatic action.

Table 2. Actions and activities against IW threats

Source: Directorate for Command, Control, Communications and Computer Systems report (J-6 report), *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, (Washington, DC: Pentagon, 1996).

[24] J-6 report, 2-98.

Based on the legal, technological and intelligence environments defined above, it is time to present the Brazilian IW doctrine in operational terms. This doctrine is formed through integrating efforts with the purpose of contributing to the achievement of Brazilian national objectives.

One of the objectives of the IW doctrine for the Brazilian military is the constitution of an information operation task force, organized to be able to execute the activities shown on table 2.

The key operational points for the total achievement of the Brazilian national objectives based on an IW doctrine, with respect to the military, are the following:

- Development of standard operational procedures for the three armed forces;
- Investment in groups of technological research and development;
- Creation of a new operation staff advisor for IW inside the Brazilian Military Planning Process;
- Centralization of matériel acquisition; and
- Development of a joint military doctrine.

The first point is fundamental to creating an adequate environment for the next transitions. Once the three armed forces establish a common pattern of procedures, the evolution for the next steps will be easier. Fundamentally, the differences are not great, but the equalization of terminology with standardized tactics, techniques and procedures is necessary. This action comprises the interchange of officers between service academies and post-commission schools, and the multinational interchange of students between foreign schools in the United States, Europe and Latin America. Also, in this proposal it is necessary to define exactly the areas of action of each force with respect to IW threats to Brazil. To achieve this purpose, a group would be organized with representatives of each armed force, and the focus of these representatives might be to define access criteria and establish the standards and specific actions for each force with the agreement of the others.

In order to give Brazil's military community the guidance and leadership required to accomplish IW integration, BRMC can create an independent IW company. This company will be responsible for the execution of all IW actions and will be formed during peacetime by platoons with essential tasks to collect and analyze information, to execute deception and psychological operations, and to execute immediate threat reaction.

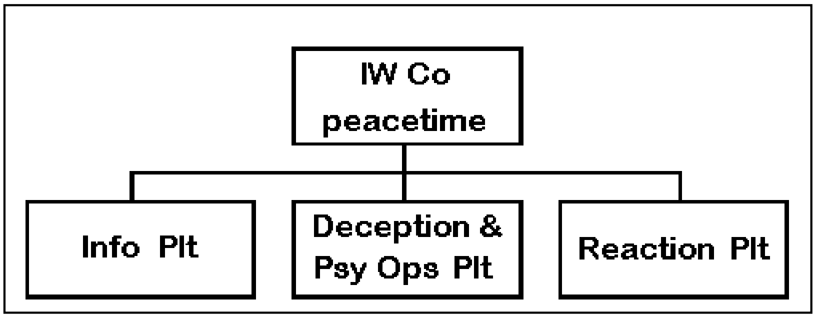

Figure 2. Information Warfare Company composition during peacetime

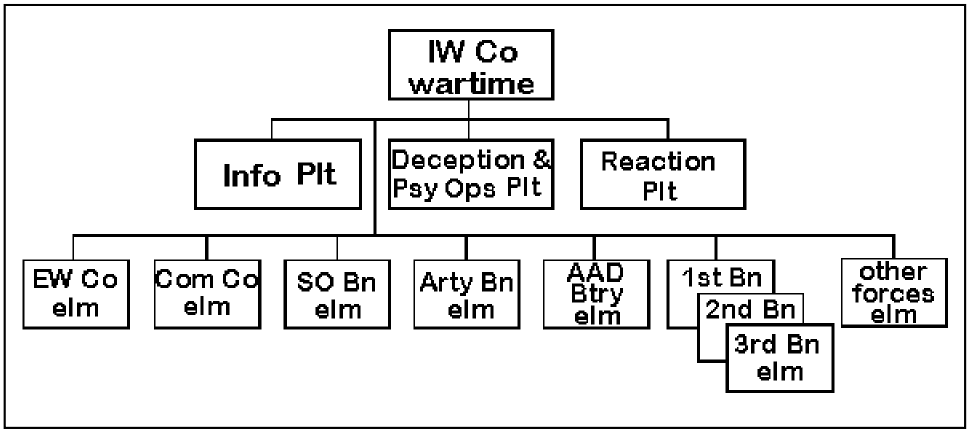

Figure 3: Information Warfare Company composition during crisis

In time of crisis, this company will be reinforced by elements from BRMC Electronic Warfare (EW Co) and Communications (Com Co) independent companies, BRMC Infantry (1st, 2nd and 3rd Bn), Artillery (Arty Bn) and Special Operations (SO Bn) Battalions, BRMC Anti-Air Defense Battery (AAD Btry) and from other friendly and multinational forces.

To complement the standardization, the establishment of an IW group for research and development is necessary to give more credibility to the proposed doctrine. It might be composed of military technicians with considerable knowledge in the technological and military doctrinal areas. The group should address the following issues, giving solutions suitable to Brazilian capabilities:

- Establish the security levels needed for a specific procedure;
- Equate the communication doctrine to the doctrinal threat levels;
- Evaluate the importance of accuracy, reliability, security and flexibility with respect to each threat level;
- Revise the threat level definitions and associate the actions to be developed in each of them with respect to the legal environment;
- Establish procedures to control the access to military databases; and
- Define the policy of security in accordance with the intelligence environment.

Brazilian Information Quality Criteria	
Accuracy	The information must be relevant to the given situation.
Usability	The information must be displayed in an easily understood format, available in time for decision and applied to the situation in focus.
Completeness	All necessary information required by the decision-maker must be presented, but only on the desired level of detail.
Security	The information must be adequately protected, when required.

Table 3: Brazilian Information Quality Criteria

Source: Directorate for Command, Control, Communications and Computer Systems report (J-6 report), *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, (Washington, DC: Pentagon, 1996).

In addition to these specific issues, the group will address all issues which will provide the secure flow of information throughout the Brazilian Information Infrastructure which ensures that every official responsible on each staff has the information and communication assets needed to accomplish the mission, in accordance with the information quality criteria of table 3.

Third, the actual Brazilian Military Planning Process considers Information Operations as part of Intelligence and Communications planning guidance. In both of them, IW is not given the attention required, and therefore a staff advisory position for IW should be created. The profile of this advisor would be a mix of technical and operational contributions. Among other considerations, in order to advise the commander in his decision-making process, the IW staff advisory office will:

- Determine the best information and communication network which provides interoperability and compatibility within all the forces;
- Evaluate the level of IW threat to which the force is exposed;

- Determine the best action to minimize the impacts caused by the threat actions;
- Determine the security chain and procedures to maintain the operation's information support ;
- Integrate the efforts of the intelligence community; and
- Suggest to the commander which Decision Support Tools will be used to filter, evaluate and analyze the mix of information received during the operation.

Despite the tools suggested above, the human element remains the essential factor to define the best decision during an operation. The experience and leadership of the commander dictates the decision-making process, and he will use his knowledge and insight to achieve the objectives. Some decision-making requirements remain subjective, and their importance can only be measured by the commander's personality. In the BRMC particular case, the IW advisor will come from the IW Company as suggested above.

To confirm the practicability of the IW staff advisor position, the Brazilian Navy's Secretary of Science and Technology believes that, "in the near future, the Brazilian Military Planning Process will have a strong technological component with considerable technical presence."[25]

The efforts made with respect to military integration will not be complete without

[25] Mario J. F. Braga (Vice-Alte), Brazilian Navy's Secretary of Science and Technology, Electronic Interview by author, 1997.

the centralization of materiel acquisition. The centralization stated here is not related to buying equipment, but to the parameters definition for quality of operation. The definition of quantity is part of centralization, too. Each force is allowed to buy the necessary equipment by itself, but with specifications defined by the acquisition centralization committee. This committee would be formed by elements of each service plus technical advisors from other governmental sectors, to ensure the interoperability of all equipment available during an operation, in strict accordance with the level of integration needed, which means without unnecessary expenses.

The Brazilian armed forces have normally operated under isolated parameters. Each of them is responsible independently for land, sea and air operations. The Navy and the Army have their own air assets, which are responsible for specific tasks for each of them. Neither force operates fixed wing aircraft, which restrains their employment on deep operations. The BRMC, which belongs to the Navy, is responsible for the projection of power from sea to shore and is prepared to hand over to the Army in the case of subsequent operations. When two or more forces train together, they operate separately, not joint. The joint doctrine is not exercised by the Brazilian military, and when it is necessary to combine efforts during one exercise, many problems occur due to the different procedures of each force. With the concrete achievement of the previous points, the establishment of a joint military doctrine will minimize the interoperability problems and will facilitate the employment of the armed forces for the maintenance of Brazilian National Objectives.

Having defined the key points for the development of the Brazilian IW doctrine, what will be the strategic implications of the adoption of this doctrine? Is it in accordance with Brazilian resources and necessities?

The strategic implications for the military segment of Brazilian society are clear. The development of a Brazilian joint military doctrine will change the actual military panorama, giving the needed integration necessary not only for the IW doctrine, but also for the interoperability of the armed forces with respect to threats to the National Defense Policy. By accomplishing the National Defense Strategy objectives, threats are neutralized and the national security guaranteed. The effort to integrate all facets of Brazilian society is fundamental to maintaining the nation's security. It is unreasonable to believe that only the IW doctrine will provide security for the nation, but it is clear that with its important tasks and cooperation, the resolution will be easier and faster.

> The feasibility and effectiveness of this project [National Drug Enforcement Program] shall be dependent, on the ability of public agencies at federal, state and local level, NGOs, patronal and labor unions to work in concert within the framework of the National System of Drug Enforcement and Prevention and the pursuit of its objectives.[26]

The strategic economic aspects cause more concern. The requirement of resources for the initial development of the proposed doctrine is not great, but after the establishment of equipment specifications in accordance with the interoperability desired, the rate of investment will increase rapidly to achieve the necessary readiness. Also, the investment in education, research and development will increase considerably after the initial doctrinal development.

IW is not the only way to control Brazil's boundaries and combat drug traffic, but it is less expensive in long-term evaluation. In the case of adoption of different ways of regional control and security of sovereignty in the Amazon region (like troop occupation

[26] Ministry of Justice Brazil.

and tax privileges to settle new cities), time and economic resources have historically been ineffective. A good example is the Transamazon Highway built in the 1970's to integrate Brazil's territory and which was abandoned due to difficulties in establishing settlements and maintaining the highway in that adverse environment.

In addition, the military force would augment to permit federal occupation of the region and, to do it, an increased budget for military purposes will be necessary. The long-term investment would be greater to establish military garrisons with its needed logistical self-sustainment.

Regional occupation, while allowing real territory control, has the disadvantage of exposing Brazilian people to undesirable external influences. If the population grievances are not seriously considered, the regional occupation might be converted into an insurgency focus, decreasing the government's influence as happened in the 1970's during the Araguaia Guerrilla.

The Brazilian information systems security strategy was developed when computers were physically and electronically isolated. It resulted in many discrepancies with respect to the new security level adopted. To adapt the Brazilian systems to the new networked world environment, the security strategy must:

- concern itself with risk management;
- consider information systems security as part of a countermeasure combined effort;
- be flexible enough to consider all variations among existing and planned systems;
- combine computer science and public key cryptography; and
- respond quickly to information technology dynamics.

This IW doctrine is an important step towards Brazilian integration into the international information community. Its integration is fundamental for the next century if Brazil intends to consolidate its relevant position in the world. The request of a permanent seat on the Security Council of the United Nations gives Brazil, beyond simple recognition, new challenges and responsibilities not of previous concern. Now, the focus of Brazilian IW doctrine implications in the world will be addressed with respect to the United States and South America.

The establishment of security information conditions within Brazilian territory permits the increase of American investment in the Brazilian economy, which represents economic and social benefits for both countries. Also, telecommunications investment opportunities are increasing with the new Brazilian privatization policy. The demand for service is great, and the necessity of a secure environment will be felt soon.

With the direct support of American leadership in the information sector, the Brazilian IW doctrine will define the paths to be adopted by other South American countries. The employment of a concrete and reliable IW doctrine will allow Brazil to lead the South American countries, spreading its doctrine and creating an adequate environment for the establishment of a military coalition between the countries. This action will permit the consolidation of the desired security condition needed for the maintenance of peace on the continent.

The Brazilian influence in South America will also create a buffer situation suitable for the world environment. Some attacks, like the one made by an Argentinean hacker against the American government[27] could be avoided if the South American

[27] J-6 report, 2-48.

countries were integrated physically, technically and logically with the same objectives of IW security as the United States.

The adoption of a new doctrine will create some unforeseeable implications, which can not be addressed in this document, mainly because this doctrine is related to a concept as subjective as IW. I believe that despite the initial coordination challenges, the adoption of the new doctrine will benefit the international community. The development of an IW doctrine should be a concern of every nation with clear objectives in the near future.

Based in the Brazilian nature, the establishment of an IW doctrine for Brazil will require input from all components of society. In a country with so many social and internal problems, it is difficult to convince the people and budget controllers of the benefits of adoption of this new technological concept, but not impossible. The military establishment must realize that the dependence upon computer systems for communication, control and weapon aiming and targeting is increasing, and needs adequate levels of security. Also, supplementary systems have to be prepared in case of failure of any system.

The IW doctrine proposed for Brazil is suitable to both peacetime and wartime, regardless of the Brazilian defensive posture. The establishment of this doctrine will require the development of procedures to be applied either in exercises or real conflicts. The system and procedures used during an exercise must forecast the worst scenario to avoid surprises during a real information operation.

The lack of knowledge in all segments of Brazilian society is the primary issue. Inside the military, the fear of computer use still exists; however, it can be foreseen and corrected in time for the realization of the doctrine. Admiral Braga, the Navy's Secretary for Science and Technology, believes that "Brazilian self-sufficiency with respect to IW will be reached within the next ten years with maintenance of the current level of effort."[28] I agree with his point of view, but I hope he has been a pessimist with his forecast.

There is no doubt that integration in all fields is the major concern for the realization of this doctrine. I strongly believe that the success of the doctrine is based upon the adoption of the proposed changes to the legal, technological and intelligence environments, and the key operational points formerly proposed.

To finish this document, I would like to present a thought of Admiral Braga, who wisely defined how future battles will be won:

> It is more important to keep the subordinates informed about what happens because it is the only way to make them engage in the effort. People are not robots! The Decision Support System does not substitute for command, however, as the military operations are necessarily contaminated by uncertainties, and the victory will tend to go to him who knows more and knows it first.[29]

[28] Braga.

[29] Braga.

BIBLIOGRAPHY

Aldrich, Richard W., Maj (USAF). *The International Legal Implications of Information Warfare*. Montgomery, AL. Airpower Journal, Vol X No. 3, 1996. URL: <http://www.cdsar.af.mil/apj/aldricha.html>. Accessed 25 August 1997.

Berkowitz, Bruce D. "Warfare in the Information Age." in *Information Age Anthology*. Ed. David S. Alberts and Daniel S. Papp, 519-544. Washington, DC, National Defense University, 1997.

Braga, Mario J. F. (Vice-Alte). Brazilian Navy's Secretary of Science and Technology. Electronic Interview by author, December 1997.

Campen, Alan D. Col. USAF (Ret), Douglas H. Dearth and R. Thomas Goodden. *CyberWar: Security, Strategy and Conflict in the Information Age*. Fairfax, VA, AFCEA International Press, 1996.

Cardoso, Fernando Henrique. *Brazilian National Defense Policy*. Washington, DC, 1996. URL: <http://www.brasil.emb.nw.dc.us/fpst10de.htm>. Accessed 2 January 1998.

Casper, E. Lawrence, Col. USA and others. *Knowledge-Based Warfare: A Security Strategy for*
the Next Century. Washington, DC, Joint Force Quarterly - number 13, 1996.

Directorate for Command, Control, Communications and Computer Systems (J-6) report. *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*. Washington, DC, Pentagon, 1996.

Graham, Bradley. "11 U.S. Military Computer Systems Breached by Hackers This Month." *The*
Washington Post, 26 February 1998, Sec. A1.

International Narcotics Control Board. *Report of International Narcotics Control Board for 1997*. Vienna, Austria, United Nations Publications, 1998. URL: <http://www.undcp.org/incb/AR/e/report.htm>. Accessed 3 January 1998.

Joint Pub 6-0 - *Doctrine of C4 Systems Support in Joint Operations*. Washington, DC,Pentagon, 1995.

Johnson, Stuart E. and Martin C. Libicki. *Dominant Battlespace Knowledge*. Washington, DC, National Defense University, 1996.

Kuehl, Dan Dr. *Defining Information Warfare*. ROA National Security Report – November 1997. Washington, DC, Defense Education Trust Fund of Reserve Officers Association of the United States, 1997.

Libicki, Martin C. *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*. Washington, DC, National Defense University, 1995.

Macgregor, Douglas A. *Breaking the Phalanx: a New Design for Landpower in the 21st Century*. Westport, CT, Praeger, 1997.

Mahnken, Thomas G. *War in the Information Age*. Washington, DC, Joint Force Quarterly - Number 10, 1996.

Maxwell, Arthur G. *Joint Training for Information Managers*. Washington, DC, National Defense University, 1996.

Mendel, William W. and Murl D. Munger. *Strategic Planning and the Drug Threat*. Fort Leavenworth, KS, Strategic Studies Institute, 1997.

Ministry of Justice Brazil. *National Drug Enforcement Program*. Brasília, DF, Ministry of Justice, 1996. URL: <http://www.brasil.emb.nw.dc.us/wpar09dr.htm>. Accessed 2 January 1998.

Molander, Roger C., Andrew S. Riddile and Peter A. Wilson. *Strategic Information Warfare: A New Face of War*. Santa Monica, CA, RAND, 1996.

Oliveira, Daílson M. de (TCol-Av-FAB). *SIPAM-SIVAM. Olhos para a Amazônia.* Montgomery, AL, Airpower Journal International - Portuguese Edition, 1995. URL: <http://www.edsar.af.mil/apj-p/poliveira.html>. Accessed 3 January 1998.

Pinheiro, Álvaro de Souza (Col-EB). *Guerrilha in the Brazilian Amazon.* Fort Leavenworth, KS, Foreign Military Studies Office, 1995.

Ryan, Donald E., Jr., LtCol USAF. *Implications of Information-Base Warfare*. Washington, DC, Joint Force Quarterly - Number 6, 1995.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. New York, NY, Thunder’s Mouth Press, 1994.

Shalikashvili, John M., Chairman of the Joint Chiefs of Staff. *Joint Vision 2010.* Washington, DC, Pentagon, 1996.

Shalikashvili, John M., Chairman of the Joint Chiefs of Staff. *National Military Strategy of the USA*. Washington, DC, Pentagon, 1997.

Slatalla, Michelle and Joshua Quittner. *Masters of Deception: the Gang that Ruled Cyberspace*. New York, NY, HarperPerennial, 1996.

Toffler, Alvin. *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*. New York, NY, Bantam Books, 1991.

Toffler, Alvin. *The Third Wave: the Classic Study of Tomorrow*. New York, NY, Bantam Books, 1981.

Toffler, Alvin and Heidi Toffler. *War and Anti-war: Making Sense of Today's Global Chaos*. New York, NY, Warner Books, 1993.

Vasconcelos, Adriana. "FH sanciona lei sobre derrubada de aviões." *O Globo on-line*, 16 Jan 1998, Sec. País. URL: <http://www.globoon.com.br/pais/19980116.htm>. Accessed 16 Jan 1998.

Whitaker, Randall, Ph.D. *Information Warfare Glossary- The Convoluted Terminology on Information Warfare*. 1997. URL: <http://www.i-war.com/glossary.htm>. Accessed 25 August 1997.